

**Kathleen M Carley, Ju-Sung Lee, David Krackhardt**  
**2002 “Destabilizing Networks” in Connections 24(3): 79-92.**

## Destabilizing Networks<sup>1</sup>

Kathleen M. Carley<sup>2</sup>

Ju-Sung Lee

David Krackhardt

*Carnegie Mellon University, Pittsburgh, Pennsylvania, USA*

*The world we live in is a complex socio-technical system. Although social, organizational and policy analysts have long recognized that groups, organizations, institutions and the societies in which they are embedded are complex systems; it is only recently that we have had the tools for systematically thinking about, representing, modelling and analyzing these systems. These tools include multi-agent computer models and the body of statistical tools and measures in social networks.*

*This paper uses social network analysis and multi-agent models to discuss how to destabilize networks. In addition, we illustrate the potential difficulty in destabilizing networks that are large, distributed, and composed of individuals linked on a number of socio-demographic dimensions. The specific results herein are generated, and our ability to think through such systems is enhanced, by using a multi-agent network approach to complex systems. Such an illustration is particularly salient in light of the tragic events of September 11, 2001.*

### WHAT CAN OUR TOOLS DO?

There are a number of ways in which our tools, both classical social network techniques and the combination of networks and multi-agent systems, can help us understand network destabilization. Before describing these, an important word of caution is needed. Network tools are clearly not a panacea and it is important that as a community we do not oversell these tools. That being said, there are at least two fundamental ways in which network statistics and measures can be brought to bear to address issues at the heart of destabilizing networks.

---

<sup>1</sup>This work was supported in part by the Office of Naval Research (ONR), United States Navy Grant No. N00014-97-1-0037, NSF IRI9633 662, Army Research Labs, NSF ITR/IM IIS-0081219, NSF KDI IIS-9980109, NSF IGERT: CASOS, and the Pennsylvania Infrastructure Technology Alliance, a partnership of Carnegie Mellon, Lehigh University, and the Commonwealth of Pennsylvania's Department of Economic and Community Development. Additional support was provided by ICES (the Institute for Complex Engineered Systems) and CASOS - the center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University (<http://www.casos.ece.cmu.edu>). The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research, the National Science Foundation or the U.S. government.

<sup>2</sup>Direct all correspondence to: Prof. Kathleen M. Carley, Dept. of Social and Decision Sciences, Carnegie Mellon University, Pittsburgh, PA 15143, Email: [kathelen.carley@cmu.edu](mailto:kathelen.carley@cmu.edu), Fax: 1-412-268-6938, Tel: 1-412-268-3225, URL: <http://hss.cmu.edu/departments/sds/faculty/carley.html>

***Location of critical individuals, groups, technologies***

Given any network, such as a communication network, or alliance structure, or monetary flow, where the nodes are individuals, groups, computers, etc., a number of network measures such as centrality or cut-points can be used to locate critical nodes. Additional measures based on an information processing view of organizations also exist for locating critical employees, redundancy, and potential weak points within groups and organizations. Many of the traditional social network measures and the information processing network measures are embedded within ThreatFinder (Carley, 2000). ThreatFinder is a computer program that uses a combination of network analysis and multi-agent modelling to determine the potential information security risk from personnel that an organization faces due to its architecture. The degree, type, and location of possible threats, such as critical employees and lack of redundancy are assessed. These "location" techniques are useful within companies to help ensure information security and are useful within and among groups and organizations in mitigating the effectiveness of networks. For example, individuals or groups with the following characteristics can be identified:

1. An individual or group where removal would alter the network significantly; e.g., by making it less able to adapt, by reducing performance, or by inhibiting the flow of information. Illustrative nodes are those high exceptionally high in centrality (Bonacich, 1987) or high in structural holes (Burt, 1992).
2. An individual or group that is unlikely to act even if given alternative information. This can be found as an individual high in centrality and Simmelian ties (Krackhardt, 1999).
3. An individual or group that if given new information can propagate it rapidly. Such individuals may be seen as gossips, innovators, or early adopters (Rogers and Shoemaker, 1971). Possible indicators are high degree centrality or high structural holes.
4. An individual or group that has relatively more power and can be a possible source of trouble, potential dissidents, or potential innovators. Individuals with relatively more power may be high in centrality (Bonacich, 1987; Brass, 1991; Brass and Burkhardt, 1992). Possible innovators may be those who are isolates or those who have moved about so much that they have broad and distributed knowledge and contacts.
5. An individual or group where movement to a competing group or organization would ensure that the competing unit would learn all the core or critical information in the original group or organization (inevitable disclosure) (Carley, 2000).
6. An individual, group, or resource that provides redundancy in the network (Carley and Ren, 2001). Measures of redundancy are available in ThreatFinder (Carley, 2000).

For the measures discussed above most can be calculated using UCINET<sup>3</sup> or the meta-network R-package package<sup>4</sup>.

***Pattern location***

Over the past few years, major advances have been made in graph level analysis. These techniques include the P\* family of tools, network level metrics (such as group and graph clustering algorithms using distance metrics such as the Hamming distance). These pattern location techniques can be used on any data that can be represented as graphs; such as, interaction or communication networks, monetary networks, inter-organizational alliances, mental models, texts, web pages, who was present at what event, and story lines. These pattern location techniques, particularly when combined with machine learning techniques, are likely to be especially powerful for locating patterns not visible to the human eye. A key to many of the detection algorithms is that they search for behavior that is different

<sup>3</sup> <http://eclectic.ss.uci.edu/~lin/ucinet.html>

<sup>4</sup> <http://legba.hss.cmu.edu/R.stuff>

from some baseline. Thus, if run on network data, The baseline might be networks, biased networks, or a sample of existing networks. For example, the following kinds of patterns or breaks in patterns can be examined:

- The basic components that account for the networks structure can be identified; e.g., the number and types of sub-groups, or the number of triads, stars, and the extent of reciprocity (Anderson, Wasserman, and Crouch, 1999; Wasserman, and Pattison, 1996).
- The central tendency within a set of networks, and the networks that are anomalous when contrasted with the other networks can be located (Banks and Carley, 1994).
- Critical differences between two or more sets of networks can be identified; e.g., are programming teams structured differently than sales teams or are managers' mental models different from subordinates (Banks and Carley, 1994; Carley and Banks, 1993; Butts and Carley, 2001). For sets of concepts, comparison techniques based on the idea of lossy integration and set theory have been used to compare two or more concept networks or mental models (Carley and Palmquist, 1992; Carley, 1997). In principle, these methods developed for text analysis could be utilized for the comparison of social networks.
- Which components in the network are structured significantly differently from the rest of the overall network? A standard approach is to locate the nodes or sets of nodes that differ significantly from other nodes on standard measures such as degree centrality, betweenness, and number of cliques. However, for extremely large networks or where only samples of data on the network exist this approach may not be feasible (processing time is excessive, space requirements are too high, or missing data is too high). Under these conditions, you can use machine learning algorithms such as simulated annealing (Kirkpatrick, Gelato and Vichy, 1983) or Bayesian updating (Butts, forthcoming; German, Carlin, Stern, and Rubin, 1995; Robert, 1994) to search through the network to locate the node or set of nodes that are highest on some criteria or best match some criteria such as excessively high or low centrality.
- Whether the existing network is coherent; i.e., what is the likelihood that there are key missing nodes or relations. One approach here is to locate the differences between an actual network and a network predicted from first principles to see where there are differences. For example, if two individuals are not interacting in the social network but should be based on the principles of relative similarity and relative expertise, then there may be hidden relations. This is one of the calculations in ThreatFinder (Carley, 2000).

#### ***What-if analysis and policy guidance***

In addition, multi-agent models of adaptive agents embedded in social networks can be used to address issues of network destabilization by providing managerial and policy guidance (Carley, forthcoming a). In a multi-agent computational program the behavior of the group or organization emerges from the actions and interactions of the agents who are members of the group or organization. Typically the agents are able to learn and adapt, although models vary widely in the extent to which the agents are cognitively realistic (Carley, forthcoming b). Few multi-agent models have more than 100,000 agents and in general the number of agents decreases as the cognitive complexity and realism of the agents increases. Multi-agent systems are typically non-linear and exhibit path dependence. Most multi-agent models have no network underpinning. In the artificial life models (Epstein and Axtell, 1997) the agents typically interact on a grid with physical proximity serving as a proxy for networks. In the most cognitively sophisticated models, such as the Soar models (Tambe, 1997), the set of interactions and so the network are predefined. However, recently, there has been a movement to combining multi-agent and network models (More and Ramanujam, 1999; Levinthal, 1997; Macy and Skvoretz, 1998; Carley, 1990; Carley and Svoboda, 1997).

